UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

November 28, 2011

Mr. Brian J. O'Grady
Vice President-Nuclear and CNO
Nebraska Public Power District
72676 648A Avenue
Brownville, NE 68321

SUBJECT: COOPER NUCLEAR STATION - CORRECTION TO SAFETY EVALUATION OF AMENDMENT NO. 238 FOR FACILITY OPERATING LICENSE NO. DPR-46 RE: APPROVAL OF CYBER SECURITY PLAN (TAC NO. ME4270)

Dear Mr. O'Grady:

By letter dated July 27, 2011 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML111801081), the U.S. Nuclear Regulatory Commission (NRC) issued Amendment No. 238 to the facility operating license for the Cooper Nuclear Station (CNS). The amendment consisted of changes to Facility Operating License No. DPR-46, in response to your application dated July 20, 2010, as supplemented by letters dated September 27 and November 30, 2010, and March 30, 2011 (ADAMS Accession Nos. ML102070034, ML102770094, ML103360041, and ML110910061, respectively).

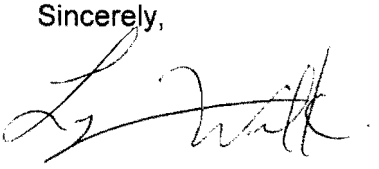
The amendment approved the cyber security plan (CSP) and associated implementation schedule, and revised Paragraph 2.C.(3) of Renewed Facility Operating License No. DPR-46 to provide a license condition to require the licensee to fully implement and maintain in effect all provisions of the NRC-approved Cyber Security Plan. The change was consistent with Nuclear Energy Institute (NEI) 08–09, Revision 6, "Cyber Security Plan for Nuclear Power Reactors."

The NRC staff has identified errors on pages 5-10, 13, and 14 of Enclosure 2 to the NRC staff's letter dated July 27, 2011. Pages 5-10 incorrectly cited section numbers that do not align with the licensee's CSP. Page 13 mentioned a "table of deviation found in Attachment 1," which does not align with the licensee's CSP. Also, page 14 incorrectly referred to another nuclear power plant in its conclusion section. Accordingly, please discard pages 5-10, 13, and 14 of Enclosure 2 to the NRC's letter dated July 27, 2011, and replace with the enclosed corrected pages. The changed portions are indicated by revision bars.

These errors, on the part of the NRC, were administrative in nature, only affected the specified pages for CNS, and do not change the NRC staff's conclusions regarding Amendment No. 238 for Renewed Facility Operating License No. DPR-46.

We regret any inconvenience caused by this error. If you have any questions, please contact me at 301-415-1377 or via e-mail at lynnea.wilkins@nrc.gov.

Sincerely,



Lynnea E. Wilkins, Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-298

Enclosure:
As stated

cc w/encl: Distribution via Listserv

ENCLOSURE

Revised pages 5-10, 13, and 14 of Enclosure 2 to

U.S. Nuclear Regulatory Commission's Letter to Nebraska Public

Power District dated July 27, 2011, re Amendment No. 238

that the licensee established adequate measures to implement and document the Cyber Security Program, including baseline security controls.

Based on the above, the NRC staff concludes that the licensee's CSP adequately establishes the Cyber Security Program, including baseline security controls.

3.2 Analyzing Digital Computer Systems and Networks and Applying Cyber Security Controls

The licensee's CSP describes that the Cyber Security Program is established, implemented, and maintained as described in Section 3.1 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3 described in RG 5.71 to:

- Analyze digital computer and communications systems and networks, and
- Identify those assets that must be protected against cyber attacks to satisfy 10 CFR 73.54(a).

The CSP submitted by the licensee describes how the cyber security controls in Appendices D and E of NEI 08-09, Revision 6, which are comparable to Appendices B and C in RG 5.71, are addressed to protect CDAs from cyber attacks.

Section 3.1 of the CSP is comparable to Regulatory Position C.3 in RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately addresses security controls.

3.3 Cyber Security Assessment and Authorization

The licensee provided information addressing the creation of a formal, documented, cyber security assessment and authorization policy. This included a description concerning the creation of a formal, documented procedure comparable to Section 3.1.1 of NEI 08-09, Revision 6.

The NRC staff concludes that the licensee established adequate measures to define and address the purpose, scope, roles, responsibilities, management commitment, and coordination, and facilitates the implementation of the cyber security assessment and authorization policy.

The NRC staff reviewed the above information and found no deviation from Section 3.1.1 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.1 in RG 5.71. Based on the above, the NRC staff concludes that the licensee's CSP adequately established controls to develop, disseminate, and periodically update the cyber security assessment and authorization policy and implementing procedure.

3.4 Cyber Security Assessment Team

The Cyber Security Assessment Team (CSAT) responsibilities include conducting the cyber security assessment, documenting key findings during the assessment, and evaluating assumptions and conclusions about cyber security threats. The CSP submitted by the licensee

outlines the requirements, roles, and responsibilities of the CSAT comparable to Section 3.1.2 of NEI 08-09, Revision 6. It also describes that the CSAT has the authority to conduct an independent assessment.

The CSP submitted by the licensee describes that the CSAT will consist of individuals with knowledge about information and digital systems technology; NPP operations, engineering, and plant technical specifications; and physical security and emergency preparedness systems and programs. The CSAT description in the CSP is comparable to Regulatory Position C.3.1.2 in RG 5.71.

The CSP submitted by the licensee lists the roles and responsibilities for the CSAT which included performing and overseeing the cyber security assessment process; documenting key observations; evaluating information about cyber security threats and vulnerabilities; confirming information obtained during tabletop reviews, walk-downs, or electronic validation of CDAs; and identifying potential new cyber security controls.

Section 3.1.2 of the CSP is comparable to Regulatory Position C.3.1.2 in RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately establishes the requirements, roles, and responsibilities of the CSAT.

3.5 Identification of CDAs

The CSP submitted by the licensee describes that the licensee will identify and document CDAs and critical systems (CSs), including a general description, the overall function, the overall consequences if a compromise were to occur, and the security functional requirements or specifications as described in Section 3.1.3 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.3 of RG 5.71, without deviation.

Based on the above, the NRC staff concludes that the licensee's CSP adequately describes the process to identify CDAs.

3.6 Examination of Cyber Security Practices

The CSP submitted by the licensee describes how the CSAT will examine and document the existing cyber security policies, procedures, and practices; existing cyber security controls; detailed descriptions of network and communication architectures (or network/communication architecture drawings); information on security devices; and any other information that may be helpful during the cyber security assessment process as described in Section 3.1.4 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.2 of RG 5.71. The examinations will include an analysis of the effectiveness of the existing Cyber Security Program and cyber security controls. The CSAT will document the collected cyber security information and the results of their examination of the collected information.

Section 3.1.4 of the CSP is comparable to Regulatory Position C.3.1.2 in RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes the examination of cyber security practices.

3.7 Tabletop Reviews and Validation Testing

The CSP submitted by the licensee describes tabletop reviews and validation testing, which confirm the direct and indirect connectivity of each CDA and identify direct and indirect pathways to CDAs. The CSP states that validation testing will be performed electronically or by physical walkdowns. The licensee's plan for tabletop reviews and validation testing is comparable to Section 3.1.5 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.1.4 of RG 5.71.

This section is comparable to Regulatory Position C.3.1.4 in RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes tabletop reviews and validation testing.

3.8 Mitigation of Vulnerabilities and Application of Cyber Security Controls

The CSP submitted by the licensee describes the use of information collected during the cyber security assessment process (e.g., disposition of cyber security controls, defensive models, defensive strategy measures, site and corporate network architectures) to implement security controls in accordance with Section 3.1.6 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3 and Appendix A.3.1.6 to RG 5.71. The CSP describes the process that will be applied in cases where security controls cannot be implemented.

The CSP submitted by the licensee notes that before the licensee can implement security controls on a CDA, it will assess the potential for adverse impact in accordance with Section 3.1.6 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3 of RG 5.71, without deviation.

Based on the above, the NRC staff concludes that the licensee's CSP adequately describes mitigation of vulnerabilities and application of security controls.

3.9 Incorporating the Cyber Security Program into the Physical Protection Program

The CSP submitted by the licensee states that the Cyber Security Program will be reviewed as a component of the Physical Security Program in accordance with the requirements of 10 CFR 73.55(m). This is comparable to Section 4.1 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.4 of RG 5.71.

Section 4.1 of the CSP is comparable to Appendix A, Section A.3.2 in RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes review of the CSP as a component of the physical security program.

3.10 Cyber Security Controls

The CSP submitted by the licensee describes how the technical, operational, and management cyber security controls contained in Appendices D and E of NEI 08-09, Revision 6, that are comparable to Appendices B and C in RG 5.71, are evaluated and dispositional based on site-specific conditions during all phases of the Cyber Security Program. The CSP describes that many security controls have actions that are required to be performed on specific frequencies

and that the frequency of a security control is satisfied if the action is performed within 1.25 times the frequency specified in the control, as applied, and as measured from the previous performance of the action as described in Section 4.2 of NEI 08-09, Revision 6.

Section 4.2 is comparable to Appendix A, Section A.3.1.6 in RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes implementation of cyber security controls.

3.11 Defense-in-Depth Protective Strategies

The CSP submitted by the licensee describes the implementation of defensive strategies that ensure the capability to detect, respond to, and recover from a cyber attack. The CSP specifies that the defensive strategies consist of security controls, defense-in-depth measures, and the defensive architecture. The submitted CSP notes that the defensive architecture establishes the logical and physical boundaries to control the data transfer between these boundaries.

The licensee established defense-in-depth strategies by: implementing and documenting a defensive architecture as described in Section 4.3 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.2 in RG 5.71; a physical security program, including physical barriers; the operational and management controls described in Appendix E of NEI 08-09, Revision 6, which is comparable to Appendix C to RG 5.71; and the technical controls described in Appendix D of NEI 08-09, Revision 6, which is comparable to Appendix B to RG 5.71.

Section 4.3 of the CSP is comparable to Regulatory Position C.3.2 and Appendix A, Section A.3.1.5 in RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes implementation of defense-in-depth protective strategies.

3.12 Ongoing Monitoring and Assessment

The CSP submitted by the licensee describes how ongoing monitoring of cyber security controls to support CDAs is implemented comparable to Appendix E of NEI 08-09, Revision 6, which is comparable to Regulatory Positions C.4.1 and C.4.2 of RG 5.71. The ongoing monitoring program includes configuration management and change control; cyber security impact analysis of changes and changed environments; ongoing assessments of cyber security controls; effectiveness analysis (to monitor and confirm that the cyber security controls are implemented correctly, operating as intended, and achieving the desired outcome) and vulnerability scans to identify new vulnerabilities that could affect the security posture of CDAs.

Section 4.4 of the CSP is comparable to Regulatory Positions C.4.1 and C.4.2 of RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes ongoing monitoring and assessment.

3.13 Modification of Digital Assets

The CSP submitted by the licensee describes how cyber security controls are established, implemented, and maintained to protect CDAs. These security controls ensure that

modifications to CDAs are evaluated before implementation, the cyber security performance objectives are maintained, and acquired CDAs have cyber security requirements in place to achieve the site's Cyber Security Program objectives. This is comparable to Section 4.5 of NEI 08-09, Revision 6, which is comparable to Appendix A, Sections A.4.2.5 and A.4.2.6 of RG 5.71, without deviation.

Based on the above, the NRC staff concludes that the licensee's CSP adequately describes modification of digital assets.

3.14 Attack Mitigation and Incident Response

The CSP submitted by the licensee describes the process to ensure that SSEP functions are not adversely impacted due to cyber attacks in accordance with Section 4.6 of NEI 08-09, Revision 6, which is comparable to Appendix C, Section C.8 of RG 5.71. The CSP includes a discussion about creating incident response policy and procedures, and addresses training, testing and drills, incident handling, incident monitoring, and incident response assistance. It also describes identification, detection, response, containment, eradication, and recovery activities comparable to Section 4.6 of NEI 08-09, Revision 6.

Section 4.6 of the CSP is comparable to Appendix C, Section C.8 of RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes attack mitigation and incident response.

3.15 Cyber Security Contingency Plan

The CSP submitted by the licensee describes creation of a Cyber Security Contingency Plan and policy that protects CDAs from the adverse impacts of a cyber attack described in Section 4.7 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3.2.7 and Appendix C.9 of RG 5.71. The licensee describes the Cyber Security Contingency Plan that would include the response to events. The plan includes procedures for operating CDAs in a contingency, roles and responsibilities of responders, processes and procedures for backup and storage of information, logical diagrams of network connectivity, current configuration information, and personnel lists for authorized access to CDAs.

Section 4.7 of the CSP is comparable to Regulatory Position C.3.3.2.7 of RG 5.71 without deviation. Based on the above, the NRC staff concludes that the CSP adequately describes the cyber security contingency plan.

3.16 Cyber Security Training and Awareness

The CSP submitted by the licensee describes a program that establishes the training requirements necessary for the licensee's personnel and contractors to perform their assigned duties and responsibilities in implementing the Cyber Security Program in accordance with Section 4.8 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3.2.8 of RG 5.71.

The CSP states that individuals will be trained with a level of cyber security knowledge commensurate with their assigned responsibilities in order to provide high assurance that

individuals are able to perform their job functions in accordance with Appendix E of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.3.2.8 of RG 5.71 and describes three levels of training: awareness training, technical training, and specialized cyber security training.

Section 4.8 of the CSP is comparable to Regulatory Position C.3.3.2.8 of RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes the cyber security training and awareness.

3.17 Evaluate and Manage Cyber Risk

The CSP submitted by the licensee describes how cyber risk is evaluated and managed utilizing site programs and procedures comparable to Section 4.9 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.4 and Appendix C, Section C.13 of RG 5.71. The CSP describes the Threat and Vulnerability Management Program, Risk Mitigation, Operational Experience Program; and the Corrective Action Program and how each will be used to evaluate and manage risk.

Section 4.9 of the CSP is comparable to Regulatory Position C.4 and Appendix C, Section C.13 of RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes evaluation and management of cyber risk.

3.18 Policies and Implementing Procedures

The CSP describes development and implementation of policies and procedures to meet security control objectives in accordance with Section 4.10 of NEI 08-09, Revision 6, which is comparable to Regulatory Position C.3.5 and Appendix A, Section A.3.3 of RG 5.71. This includes the process to document, review, approve, issue, use, and revise policies and procedures.

The CSP also describes the licensee's procedures to establish specific responsibilities for positions described in Section 4.11 of NEI 08-09, Revision 6, which is comparable to Appendix C, Section C.10.10 of RG 5.71.

Section 4.10 of the CSP is comparable to Regulatory Position C.3.5, Appendix A, Section A.3.3, and Appendix C, Section C.10.10 of RG 5.71 without deviation. Based on the above, the NRC staff concludes that the licensee's CSP adequately describes cyber security policies and implementing procedures.

3.19 Roles and Responsibilities

The CSP submitted by the licensee describes the roles and responsibilities for the qualified and experienced personnel, including the Cyber Security Program Sponsor, the Cyber Security Program Manager, Cyber Security Specialists, the Cyber Security Incident Response Team (CSIRT), and other positions as needed. The CSIRT initiates in accordance with the Incident Response Plan and initiates emergency action when required to safeguard CDAs from cyber security compromise and to assist with the eventual recovery of compromised systems. Implementing procedures establish roles and responsibilities for each of the cyber security roles

implementation date, shall be in accordance with the implementation schedule submitted by the licensee and approved by the NRC. All subsequent changes to the NRC-approved CSP implementation schedule will require prior NRC approval pursuant to 10 CFR 50.90.

3.23 Revision to License Condition 2.C.(3)

By letter dated July 20, 2010, the licensee proposed to add a paragraph to Paragraph 2.C.(3) of Renewed Facility Operating License No. DPR-46 for CNS to provide a license condition to require the licensee to fully implement and maintain in effect all provisions of the NRC-approved CSP. The NRC staff modified the proposed wording of the license condition described in the licensee's submittal dated July 20, 2010, and the licensee agreed with the revised license condition proposed by the NRC staff.

The following paragraph is added to Paragraph 2.C.(3) of Renewed Facility Operating License No. DPR-46 for CNS:

> NPPD shall fully implement and maintain in effect all provisions of the Commission-approved cyber security plan (CSP), including changes made pursuant to the authority of 10 CFR 50.90 and 10 CFR 50.54(p). The NPPD CSP was approved by License Amendment No. 238.

Based on the information in Section 3.0 of this safety evaluation and the modified license condition described above, the NRC concludes this is acceptable.

4.0 DIFFERENCES FROM NEI 08-09, REVISION 6

The NRC staff notes the following additional differences between the licensee's CSP (ADAMS Accession No. ML110910061), and NEI 08-09, Revision 6:

- In Section 3.1, "Scope and Purpose," the licensee clarified the definition of important-to-safety functions, consistent with SRM COMWCO-10-0001.
- In Section 3.21, "Document Control and Records Retention and Handling," the licensee clarified the definition of records and supporting documentation that will be retained to conform to the requirements of 10 CFR 73.54.
- In Section 3.22, "Implementation Schedule," the licensee submitted a revised implementation schedule, specifying the interim milestones and the final implementation date, including supporting rationale.

The NRC staff concludes that all of these deviations are acceptable as discussed in the respective sections of this safety evaluation.

5.0 STATE CONSULTATION

In accordance with the Commission's regulations, the Nebraska State official was notified of the proposed issuance of the amendment. The State official had no comments.

6.0 ENVIRONMENTAL CONSIDERATION

The amendment changes a requirement with respect to installation or use of a facility component located within the restricted area as defined in 10 CFR Part 20. The NRC staff has determined that the amendment involves no significant increase in the amounts, and no significant change in the types, of any effluents that may be released offsite, and that there is no significant increase in individual or cumulative occupational radiation exposure. The Commission has previously issued a proposed finding that the amendment involves no significant hazards consideration, and there has been no public comment on such finding published in the *Federal Register* on October 12, 2010 (75 FR 62602). Also, this amendment relates to safeguards matters and does not involve any significant construction impacts and relates to changes in recordkeeping, reporting, or administrative procedures or requirements. Accordingly, the amendment meets the eligibility criteria for categorical exclusion set forth in 10 CFR 51.22(c)(9), (10), and (12). Pursuant to 10 CFR 51.22(b), no environmental impact statement or environmental assessment need be prepared in connection with the issuance of the amendment.

7.0 CONCLUSION

The NRC staff's review and evaluation of the licensee's CSP was conducted using the staff positions established in the relevant sections of RG 5.71. Based on the NRC staff's review, the NRC concludes that the licensee addressed the relevant information necessary to satisfy the requirements of 10 CFR 73.54, 10 CFR 73.55(a)(1), 10 CFR 73.55(b)(8), and 10 CFR 73.55(m), as applicable, and that the licensee's Cyber Security Program provides high assurance that digital computer and communication systems and networks associated with the following are adequately protected against cyber attacks, up to and including the DBT as described in 10 CFR 73.1. This includes protecting digital computer and communication systems and networks associated with: (i) safety-related and important-to-safety functions; (ii) security functions; (iii) emergency preparedness functions, including offsite communications; and (iv) support systems and equipment which, if compromised, would adversely impact SSEP functions.

Therefore, the NRC staff concludes that the information contained in this CSP to be acceptable and upon successful implementation of this program, operation of the Cooper Nuclear Station will not be inimical to the common defense and security. The Commission has concluded, based on the considerations discussed above, that: (1) there is reasonable assurance that the health and safety of the public will not be endangered by operation in the proposed manner, (2) such activities will be conducted in compliance with the Commission's regulations, and (3) the issuance of the amendment will not be inimical to the common defense and security or to the health and safety of the public.

We regret any inconvenience caused by this error. If you have any questions, please contact me at 301-415-1377 or via e-mail at lynnea.wilkins@nrc.gov.

Sincerely,

/RA/

Lynnea E. Wilkins, Project Manager
Plant Licensing Branch IV
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

Docket No. 50-298

Enclosure:
As stated

cc w/encl: Distribution via Listserv

DISTRIBUTION:
PUBLIC
LPLIV Reading
RidsAcrsAcnw_MailCTR Resource
RidsNsirDsp Resource
RidsNrrDorlDpr Resource
RidsNrrDorlLpl4 Resource
RidsNrrPMCooper Resource
RidsNrrLAJBurkhardt Resource
RidsOgcRp Resource
RidsRgn4MailCenter Resource
PPederson, NSIR/DSP/ISCPB
RSpitzberg, NSIR/DSP/ISCPB

ADAMS Accession No.: ML112930245

OFFICE	NRR/LPL4/PM	NRR/LPL4/LA	NSIR/DSP/ISCPB/BC	NRR/LPL4/BC	NRR/LPL4/PM
NAME	LWilkins	JBurkhardt	CErlanger	MMarkley	LWilkins
DATE	10/21/11	10/21/11	10/31/11	11/28/11	11/28/11

OFFICIAL RECORD COPY